# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 10-06-2016 | Masters Thesis | 27-07-2015 to 10-06-2016 |

**4. TITLE AND SUBTITLE**

OFFENSIVE CYBER OPERATIONS:
THE NEED FOR A POLICY TO CONTEND WITH THE FUTURE

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Lt Col Brian D. Sidari, USAF

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

National Defense University
Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd
Norfolk, VA. 23511-1702

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

**Approved for public release, distribution is unlimited.**

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The United States holds a unique position in the world to capitalize on a globally interconnected information and communications infrastructure which is ingrained into every corner of society, providing conduits for public safety, the economy, and national security. Technology drives change and the evolution of daily interactions and offers endless opportunities, but these are fraught with vulnerabilities. Make no mistake that cyberspace, while not new, is the battlefield for future conflict. China, Russia, and North Korea have been implicated in compromising the systems and networks of the United States government and private corporations. These intrusions are not the first, and certainly will not be the last to effect the United States. An excellent example of an offensive cyber operation is the Stuxnet malicious virus which attacked the Iranian nuclear program. Stuxnet demonstrated that offensive cyber, when integrated with the other instruments of national power can create the time and space required for the international community to deal with a potentially nuclear Iran. The United States has been averse to discuss offensive cyber operations in the public domain. While there are numerous policy documents and senior administration statements that relate to cyberspace defense, the time has come for the United States to declare that it will conduct offensive cyber operations.

**15. SUBJECT TERMS**
Cyber, Policy, Military, Threat, Technology, Technological

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Director of JAWS |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED/ UNLIMITED | 49 | 19b. TELEPHONE NUMBER *(include area code)* 757-443-6301 |

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL


# OFFENSIVE CYBER OPERATIONS:
# THE NEED FOR A POLICY TO CONTEND WITH THE FUTURE

by

Brian D. Sidari

Lieutenant Colonel, United States Air Force

*Intentionally Left Blank*

OFFENSIVE CYBER OPERARTIONS:

THE NEED FOR A POLICY TO CONTEND WITH THE FUTURE

By

Brian D. Sidari

Lieutenant Colonel, United States Air Force

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work as documented in footnotes.

Signature: _____
BRIAN D. SIDARI, Lt Col, USAF
4 April 2016

Thesis Advisor:

Signature: _____
STERLING M. PAVELEC, Ph.D.
Thesis Advisor

Approved by:

Signature: _____
KEVIN C. THERRIEN, Colonel, USAF
Secondary Thesis Advisor

Signature: _____
PETER E. YEAGER
Colonel, U.S. Marine Corps
Director, Joint Advanced Warfighting School

*Intentionally Left Blank*

## Abstract

The United States is in a unique position in the world to capitalize on a globally interconnected information and communications infrastructure which is ingrained into every corner of society and provides a conduit for public safety, the economy, and national security. Technology drives change and the evolution of daily interactions and offers endless opportunities, but these are fraught with vulnerabilities. Make no mistake that cyberspace, while not new, is the battlefield for future conflict

The United States has experienced multiple high profile cyberattacks in the last three years. China, Russia, and North Korea have been implicated in compromising the systems and networks of the United States government and private corporations. These intrusions are not the first, and certainly will not be the last to affect the United States. However, official U.S. responses have been limited to purely law enforcement responses and have had minimal deterrent effect.

The United States requires offensive cyber capabilities, and the doctrine and the theory to guide their employment. An excellent example of an offensive cyber operation is the Stuxnet malicious virus which attacked the Iranian nuclear program. The natural response from some corners of the Department of Defense is one that cyber alone can have an immediate effect on an adversary. Stuxnet demonstrated that offensive cyber, when integrated with the other instruments of national power, can create the time and space required for the international community to deal with a potentially nuclear Iran.

There are numerous policy documents and senior administration statements that relate to cyberspace defense, but there has been a deafening silence with regard to offensive cyber capabilities. The United States has been averse to discuss offensive cyber operations in the public domain and has rarely spoken about such operations for fear of leading to an escalation of cyberattacks. The time has come for the United States to declare that it will conduct offensive cyber operations.

Acknowledgements

I would like to take this opportunity to acknowledge Dr. Sterling Pavelec, my student and thesis advisor. I thoroughly enjoyed the numerous conversations regarding current world events and United States domestic issues. While I felt prepared to argue my point of view, I always left your office questioning my beliefs. As I reflect upon back on our conversations, I'm not sure I enjoyed you challenging my logic and reasoning, but I definitely walked away with a greater appreciation of the issue. Your passion for history and the future of warfare is bar none, and your students past, present, and future are lucky to have been and to be challenged.

.

Table of Contents

# CHAPTER 1: INTRODUCTION

In the past three years there have been several high profile cyber related intrusions conducted by China, Russia, and North Korea. In each case, these events have captured the attention of the United States public due the nature of the compromise. The compromised systems and networks have resided in the White House, the Office of Personnel Management, and the Joint Chiefs of Staff. However, these were not the first times that these systems have been compromised and surely will not be the last. The United States government responded to each of these incidents in a purely law enforcement fashion. This limited response has thus far had minimal deterrent effect and raises a serious question regarding exactly what the United States policy is regarding cyberspace. A clearly articulated cyberspace policy that informs other nations and non-state actors benefits both defensive and offensive cyber operations.

According to multiple news sources, it was reported that in May 2015 that the Peoples Republic of China had hacked into and compromised the network and databases of the Office of Personnel Management and stole the personnel records of 21 million individuals, some of which included those with security clearances across the United States government. There have been a number Congressional hearings to ascertain the extent of this breach, and government actions to secure the network, but to date the response to this case of cyber espionage has been limited. Additionally, in July 2015, the unclassified email network of the Joint Chiefs of Staff was taken offline and rendered inoperable due to a complex cyberattack. The Chairman of the Joint Chiefs of Staff, General Martin E. Dempsey, stated in testimony that Russia was the responsible actor,

but no United States response was made public. In the final example, in 2014 the North Korean government conducted cyber operations against Sony Pictures Entertainment to coerce the company not to release *The Interview*, a motion picture whose plot was the assassination attempt of the North Korean leader Kim Jong Un.[1]

Kim Zetter, in her book, *Countdown to Zero Day*, chronicles the full scope of the Stuxnet virus from the initial discovery on Iranian computer systems to the efforts of the various computer security firms that dissected the source code to gain a greater understanding of the developer, intended target, and intent. This detailed account of the discovery of a cyber weapon, introduced the general public to the first known use of a cyber capability creating a kinetic effect, and illustrated the unlimited potential cyber weapons can and will play in the future of warfare[2].

The examples above will be discussed in detail on the potential and breadth of cyberattacks against both government and civilian networks and infrastructure. It can be argued that in each instance the cyberattack produced the desired effect to the individual country or actor and showed the value of cyber. As a result, the threat will continue to grow. The United States has been averse to discussing offensive cyber operations in the public domain and has rarely spoken about such operations. This research focuses primarily on publically accessible information to ensure a common framework of understanding and garner attention to the need for an offensive cyber policy.

[1] Department of Defense, Office of the Secretary of Defense, *DoD Cyber Strategy*. April 2015, (Washington, DC:, 2015),. pg 2.
[2] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Crown, 2014), pg 369-370.

## CHAPTER 2: BACKGROUND

### What is Cyberspace?

The global community has grown ever more reliant upon everyday use of mobile communications, computers, and the internet to conduct day-to-day business. Additionally, the ever-increasing interdependence of closed networks to the open internet with its associated vulnerabilities has sparked a growth in the number and complexity of cyberattacks. National infrastructure, the world's financial system, global commerce, and governmental operations, to include military operations and national security information, reside in databases on servers which are connected and online.[1] This globally interconnected information and communications infrastructure is ingrained into every corner of society and provides a conduit for public safety, the economy, and national security. Technology drives change and the evolution of computers and networks is an area of rapid and dramatic growth, with processing capacity doubling every two years, according to Moore's law. These changes present endless opportunities but are also wrought with vulnerabilities. Make no mistake that cyberspace, while not new, is the battlefield for future conflict.

In 2011, the Department of Defense recognized and declared that cyberspace was the fifth warfighter domain. Unlike the ground, sea, air, and space domains, cyber is a purely man-made, dynamic, virtual environment of information and interactions between the world's people.[2] Cyberspace seamlessly crosses into the other warfighting domains, as

[1] Michael Gervais, "Cyber Attacks and the Laws of War", *Berkley Journal of International Law,* Vol. 30, No. 2 (December 2012), pg 526.
[2] Executive Office of the President of the U.S., *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure,* (Washington D.C., 2009), pg i-iv.

there are no known geographic or recognized boundaries.[3] Unlike the other four domains in which physical objects exist throughout, in the cyber domain, it is the ones and zeros, the digital information is moving. To defend cyber as a domain, it must be viewed as an operational environment, just like air, land, sea, and space. The extent to which the cyber domain differs from the other domains represents an evolution of modern military thinking and a challenge for United States senior leaders and military commanders on the application of the rules of engagement, doctrine, and policy. Major General Brett T. Williams argues that cyber offers an additional environment to exercise the elements of national power.[4] The ability for commanders to exploit and gain an advantage against both state and non-state actors is a force multiplier and should be used in meeting the objectives of and the protection of the national interests of the United States.

However, Dr. Martin Libicki disagrees with and challenges the Department of Defense's declaration of cyberspace as a new and separate warfighting domain. He questions the purpose, and intended benefit of labeling cyberspace as a domain.[5] Unlike the other domains, which are clearly defined and easily understandable, cyberspace is basically a capability or weapon much in the same fashion as a nuclear weapon. There is not a separate defined domain to deal with nuclear-related issues, but there are capabilities such as inter-continental ballistic missiles, nuclear capable bomber aircraft, ballistic missile submarines, and associated command and control facilities, which operate in, through, and from the other four warfighting domains. The vulnerability of

[3] Sean Brandes, "The Newest Warfighting Domain: Cyberspace." *Synesis: A Journal of Science, Technology, Ethics, and Policy* Vol., No. 4 (January 2013), pg 91.
[4] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations." *JFQ: Joint Force Quarterly*, no. 73, 2014, pg 13.
[5] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain." I*/S: A Journal of Law and Policy for the Information Society* Vol.8, No.2, (Fall 2012), pg 325-340.

systems or networks to attacks from cyber capabilities is a direct result of the weakness of the system. To effectively defeat a cyberattack, one needs only to apply a simple routine software patch which changes the features of the system and erases the vulnerability. To think of cyberspace as a domain tends to convert the problems associated with operating in cyberspace, to the thinking which is shaped by the associated experiences of the other four older domains.[6] It is normal in dealing with new concepts and ideas to revert back to individual experience in an effort to help grasp and deal with the associated issues. In an effort to organize, train, and equip the force, the Department of Defense, with United States Cyber Command as lead, is developing capabilities to defend against attacks and conduct offensive operations in cyberspace. History has shown that advancements in technology are adapted into the thinking, capabilities, and conduct of war. Cyber is an evolution in warfare.

## Is Cyber Really War?

It is important to start any discussion about cyber war by defining both the nature and the character of war in order to understand how they interact. Clausewitz defines war as the use of force to impose one's will upon an enemy, reducing the will to resist.[7] Simply stated, the purpose of a state to go to war is to impose its will on another state or non-state actor. The nature of war does not change and remains an inherently violent human endeavor which pits combatants against each other to achieve the political aims of the state. The character of war is the synchronized, intentional, and calculated employment

[6] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain." I*/S: A Journal of Law and Policy for the Information Society* Vol.8, No.2, (Fall 2012), pg 325-340.
[7] Carl von Clausewitz, *On War*, translated by Michael Howard and Peter Paret, Princeton: Princeton University Press, 1976, pg 75-89.

of the instruments of national power to meet a defined end-state. The character of war is constantly changing due to the complexity of the strategic environment, the expanded use of technology, and the political commitment of the state to stay the course. Zetter, Clark, and Libicki contend that all nations or non-state actors engage in cyber war. However, in most cases, the actions which are being described should be categorized as intelligence, espionage, sabotage, or financial crime; not war as defined above.

If there is one term overused when discussing cyber, it would be war. The United States has had wars against terrorism, a tactic, against poverty, a status, and against drugs a non-living enemy. The use of the "war" concept has a deep rooted psychological meaning, it elicits passion and emotion, and it is instrumental in mobilizing a population to support. American politicians and citizens can comprehend when soldiers are deployed or enemy targets are destroyed, but there is a lack of clear understanding on the potential of cyber capabilities and the specific operations that create the desired outcomes in support of the national interests of the United States. Cyber offers an asymmetric way to counter significant conventional military advantages. During armed conflict the most likely course of action from an adversary will be a cyberattack to create some type of physical damage. Conversely, intelligence operations or espionage are most likely outside of armed hostilities. The United States needs to increase the integration and use of cyber capabilities into joint operations which will continue the evolution and posture the country to meet future challenges in the cyberspace domain.

The United States military will conduct cyber operations in support of operational and contingency plans, and looks to further integrate cyber into future joint operations.[8] The

[8] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations." *JFQ: Joint Force Quarterly* No. 73 (April 2014), pg 13.

vague and unanswered question remains: What are the trigger events that will necessitate an offensive cyber response? While there are debates on the advantages that cyber provides to the nation, the largest seam is the lack of a clear whole of government synchronized national policy. The next chapter will examine some of the current policies and strategies.

## CHAPTER 3: BIG THREE U.S. CYBER STRATEGIES

There is a general lack of effective United States whole of government policy regarding the use of cyber power. There have been numerous cyber-related reviews across the United States government throughout the years that have sought to frame the problem and provide a framework for operating in cyberspace. I will examine three current strategy and policy documents to help highlight the conflicting message they provide.

### The White House

In 2008, The Executive Office of the President undertook a comprehensive review to assess United States policies and governance frameworks for cybersecurity. While this review produced a comprehensive and deep look at the state of cyber initiatives across the government, it also looked for those interconnections between the government and civilian touch points. The cybersecurity review declared that it is the fundamental responsibility of the United States government to address the nation's strategic vulnerabilities in cyberspace, and specifically mentioning the use of force.[1] The major issue with the cybersecurity policy review is that it became outdated the moment that the final report was printed. The review detailed that cybersecurity is a whole of Government issue and that each government department and agency has a responsibility for implementing the review's recommendations. However, to have utility, any policy

[1] Executive Office of the President of the U.S., *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure,* (Washington D.C., 2009), pg i-iv.

that addresses cyber needs to be continually updated to keep pace with the rapidly changing technological evolution, and primarily forced both the Departments of Homeland Security and Defense to capture their strategy for dealing with cyber-related issues. While a start, the Government Accountability Office, in a 2013 report stated, "there is no single document that comprehensively defines the nation's cybersecurity strategy. Instead various policies developed over the span of more than a decade have contributed to the changing circumstances or the assigning of new responsibilities to various organizations."[2]

It can be argued that the United States has the necessary resources in personnel, technology, and dollars, to have a credible and effective offensive cyber capability. Numerous statements have been made which touch on the fringes of acknowledging that the United States will conduct offensive cyber operations in support of its national interests. The White House, in releasing the International Strategy for Cyberspace in 2011, stated the United States would use all necessary means, as well as exhausting all options before consideration on the user of military force to respond to cyber threats.[3] The Department of Defense followed up in June of the same year with the Strategy for Operating in Cyberspace, which stated that the United States reserved the right to act to defend the country and its interests.[4] Driving home the point of offensive capabilities, then Secretary of Defense Leon Panetta, in remarks covering cybersecurity to Business Executives in New York in 2012, stated that the department has developed the capability

---

[2] U.S. Government Accountability Office, *"Cybersecurity: national strategy, roles, and responsibilities need to be better defined and more effectively implemented"*, U.S. Government Accountability Office. (Washington D.C., 2013), pg 3-15.
[3] The Center for Strategic and International Studies; *U.S. Cyber Deterrence Declaratory Policies*, http://csis.org/images/stories/tech/151214_Cyber_Deterrence_Declaratory_Policies.pdf, (accessed December 22, 2015).
[4] Ibid.

to conduct offensive operations to counter threats to the interests of the United States.[5] These statements are the anomaly, since there is a general reluctance of senior United States leaders to categorically state the policy of the use of cyber in an offensive role. The fact that the United States has options to conduct offensive cyber operations requires a clear policy statement to this fact.[6]

## Department of Homeland Security

The Department of Homeland Security released a *Blueprint for a Secure Cyber Future* in November 2011. It aimed to codify a way ahead to create opportunities for a safe, secure, and resilient cyber environment. The document is focused first and foremost on defense, specifically, online crime and theft including the theft of intellectual property. The fallacy of a secure cyber environment is compounded by the fact that the nation's critical infrastructure is owned, operated, and maintained by the private sector. Resiliency is a word that has been grossly overused as of late, but in essence, it is to operate in both denied and degraded environments. These are lofty goals for any organization, but the vast span of responsibility of the department makes executing this strategy a Sisyphean challenge.

The department's strategy declares that it has the sole responsibility for securing cyberspace. This is a bit disingenuous. While DHS does have the responsibility for ensuring security for government users, the Department of Defense has responsibility and

[5] Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*, New York, NY. October 2012.
[6] David C. Gompert and Martin E. Libicki. "Waging Cyber War the American Way." *Survival* Vol. 57, No. 4 (July 2015), pg 8-9.

authority for security over its various networks. While cybersecurity is a shared responsibility, DHS assumes enormous risk without an effective enforcement mechanism to ensure those with connections to cyberspace have implemented the appropriate security protocols. To further compound a security nightmare, DHS has to work with Federal, State, Local, Tribal, and Private Entities, all of whom have competing interests and varying resources to implement security.[7]

An additional area of focus in the departments' strategy is that of innovation. The prosperity that the United States enjoys is based on a capability that was born of innovation. The people, corporations, and governments that use cyberspace have expanded the physical capacity as well as developed processes to gain efficiencies in the conduct of day to day interactions, and in the process have created revolutionary tools and systems that continue to harness the power of cyberspace. Innovation has moved the nation further into the information age and continues to expand and change it. However, and most importantly, additional emphasis is being placed in the area of defense which has the added benefit of identifying vulnerabilities in both hardware and software, which can be exploited for offensive purposes. The department is experimenting with big data and analytic tools aiming to create knowledge that will provide decision quality situational awareness, and the associated processes to enable rapid response and adaptation to defeat cyberattacks. However, this requires coordination and synchronization, which is the linkage to the Department of Defense.

[7] Department of Homeland Security, Office of the Secretary of Homeland Security, *Blueprint for a Secure Cyber Future*, November 2011, (Washington, D.C., 2011), pg i-v.

The Department of Defense is closely tied to the majority of the mission areas of DHS. The intrusion detection software that resides on government networks was developed by the Department of Defense and was modified for DHS use. Additionally, the attribution process of determining the origin and scope of a cyberattack falls to the Intelligence Community, and the expertise of the professionals at the National Security Agency. Furthermore, daily communication concerning the changing cyber threat picture is shared with DHS to ensure the department has the most current and accurate emerging threat information. I do not intend to paint this relationship in a negative light, but merely state that cybersecurity is a shared responsibility.

The *Blueprint for a Secure Cyber Future* is a starting point. It captures numerous higher level policy documents as well as expertise from throughout the government in its formulation. The theme of defense is resident throughout the document, but there would be benefit to clearly articulating that the United States has an offensive cyber capability when responding to cyberattacks. Furthermore, to declare that to use these offensive capabilities at a time and place of its choosing should result in producing a deterrent effect. The *Blueprint for a Secure Cyber Future* is nothing more than a starting point, and it shares many of the same issues with the White House Comprehensive Cyber Policy Review apply; they are static and were outdated the moment they were printed.

## The Department of Defense

Released in April of 2015, the Department of Defense *Cyber Strategy* continues the progress made in the previous documents that govern operations in cyberspace. Since the

initial declaration of cyber as the fifth warfighting domain, the department has made significant investments in infrastructure, capabilities, personnel, and organization. Both offensive and defensive cyber capabilities have been integrated in military operations in Iraq and Afghanistan with great success.[8] However, there is additional work to be done.

The strategy identifies three primary missions in cyberspace. First, is the defense of DoD networks, systems, and information. The second, is to be prepared to defend the United States and its interests against cyberattacks of significant consequence. The final mission is, when directed by the President or Secretary of Defense, the military must be able to provide integrated cyber capabilities to support military operations and contingency plans.[9]

The Department of Defense has developed doctrine and operational concepts for the use of offensive cyber operations, which are embedded in the existing structure and obey rules that apply to military and intelligence operations.[10] Secretary Carter is explicit that the purpose of the strategy is to bolster cyber defenses while increasing the deterrence posture.

There are numerous issues associated with the second mission area of being prepared to defend against cyberattacks of significant consequence, specifically the intergovernmental coordination that would be required with the Department of Homeland Security, which was highlighted in the 2013 General Accountability Office report. The Cybersecurity Policy review and the Department of Defense Cyber Strategy each

---

[8] Shane Harris, @War: *The Rise of the Military-Internet Complex*, (New York: Houghton Mifflin Harcourt, 2014), pg 4-7.
[9] Department of Defense, Office of the Secretary of Defense, *DoD Cyber Strategy*. April 2015, (Washington, D.C., 2015), pg i-iv.
[10] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations." *JFQ: Joint Force Quarterly* No. 73 (April 2014), pg 17.

highlight defense; the glaring hole in both documents is the lack of a comprehensive strategy with clear lanes of responsibility that address offensive cyber operations.[11]

The 2015 strategy also continued to carry the same theme as the 2011 version. The department will conduct operations in the cyber domain with a focus on restraint, respecting human life, and limiting the destruction of property.[12] These caveats draw a correlation to the Law of Armed Conflict and how they are applied to the other warfighting domains. It is standard procedure to take significant caution, and pause is given when conducting operations to ensure that United States and International law are adhered to, proportionality is applied, and finally that collateral damage is limited. A byproduct of declaring cyber a domain is the concept of inherent self-defense, that if attacked or with indications of a pending attack, the United States will conduct offensive operations to thwart the attack.

Gombert and Libicki argue that the United States lacks a cohesive offensive cyber policy which would support both defense and deterrence options.[13] The parallel is drawn to nuclear weapons and the stated United States policy of mutually assured destruction. However, when formulating potential options for an offensive cyber policy, it is helpful to refer to the other warfighter domains for insight.

There is not a codified United States policy for the conduct of offensive operations for air, ground, sea, and space. The lack of an offensive policy for the other domains has not

---

[11] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations." *JFQ: Joint Force Quarterly* No. 73 (April 2014), pg 6.
[12] Department of Defense, Office of the Secretary of Defense, *DoD Cyber Strategy*. April 2015, (Washington, D.C., 2015), pg i-iv.
[13] David C. Gombert and Martin E. Libicki, "Waging Cyber War the American Way." *Survival* Vol. 57, No. 4 (July 2015), pg 14.

impeded offensive operations and has not led other nation states to challenge this lack of policy. In testimony before Congress the head of the National Security Agency and United States Cyber Command, Admiral Michael S. Rogers testified that the ability of the United States to deter computer attacks is not working, and consideration needs to be given to boosting the military's offensive cyber capability. "The threat is growing and the intent is not only to disrupt, but also establish a presence in our networks. The effort to develop and make public offensive cyber capabilities are an important aspect of defense."[14] The evidence indicates that a policy purely focused on defense is not working to deter either cyber espionage by our adversaries or cybercrime conducted by non-state actors.

[14] Ellen Nakashima, "Cyber chief: Efforts to deter attacks against the U.S. are not working", Washington Post, 19 Mar 2015, https://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html (accessed: October 20, 2015).

## CHAPTER 4: HACKS
## OFFICE OF PERSONNEL MANAGEMENT

*"Does the size of the operation change the nature of it?" Senior Intelligence Official*[1]

Labeled as the worst data breach in American history, the Chinese cyber intrusion of the Office of Personnel Management network has led to the compromise of sensitive personal information of 22 million citizens.[2] The personal data that was stolen included the information on past, present, and future employees of the federal government. Additionally, the data included security clearance questionnaire forms and polygraph results that are fundamental to the granting of a clearance to classified national security information. The acknowledgement of the scope and size of the data stolen was unprecedented, and created a media and Congressional firestorm during the summer of 2015.

The House Oversight Committee held numerous committee hearings to ask tough questions to the Director and the Chief Information Officer from the Office of Personnel Management, and the Chief Information Officer from the Department of Homeland Security to ascertain the details, including the size and scope, actions undertaken to secure the network, the actions to notify those citizens affected. The hearings, at times contentious, provided critical details to the public which highlighted a major failure of OPM to adopt the basic cybersecurity practices of encrypted data storage, network

[1] Kellan Howell, "U.S. will retaliate against China for OPM hacks", *Washington Times*, August 1, 2015, www.washingtontimes.com/news/2015/aug/1/us-will-retaliate-against-china-for-opm-hacks/ (accessed October 15, 2015).
[2] Jason Chaffetz, "The Breach We Could Have Avoided", *The Hill*, 19 September 2015, https://oversight.house.gov/op-ed/the-breach-we-could-have-avoided/, (accessed October 5, 2015).

intrusion scanning, and the maintenance of outdated information technology systems, which led to strong calls for the U.S. to respond to those responsible for conducting the intrusion.

The Obama Administration was in a quandary. The Director of National Intelligence, Mr. James R. Clapper and Admiral Michael S. Rogers the Head of the National Security Agency had determined that the Peoples Republic of China was the responsible actor. The options available to respond were extremely limited, and would have to be well thought out to limit repercussions. Chinese President Xi Jinping was scheduled to make his first state visit to the United States in September. The Chinese cyber hack broke new ground in how the administration chose to deal with cases of espionage.[3] To further complicate a response, China has a robust cyber capability, a formidable military, and an economy that is interwoven into the economy of the United States.

The Administration had experience in responding to cyberattacks after the North Korean hack of Sony Picture. However, the difference this time around was the threat that a response could elicit an escalation of cyberattacks between the two countries.[4] Any decision had to have the effect of deterring the Chinese to conduct additional cyber operations against the United States. The Administration's response was to publicly identify that China was responsible, which the Chinese Foreign Ministry vehemently denied.[5]

---

[3] David E. Sanger, "U.S. Decides to Retaliate Against China's Hacking", *The New York Times*, July 31, 2015, http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html (accessed September 5, 2015).
[4] Ibid.
[5] Devlin Barrett, Danny Yadron, and Damian Paletta, "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say", *The Wall Street Journal*, June 5, 2015,

President Obama and Xi Jinping did agree during their meetings to work on the issue of cybersecurity. First, the United States and China agreed to work together to provide information of malicious cyber activity, consistent with respective national and international law.[6] Second, it was agreed that neither nation would engage in or knowingly support the theft of intellectual property. Next, they reaffirmed their commitment to establish norms and behavior in cyberspace. Finally, a high-level joint dialogue mechanism was agreed to address cybercrime and related issues, which would meet on a bi-annual basis.[7] The issues of cyber related intelligence operations was not discussed to ensure the United States did not tie its own hands in future endeavors. Time will tell if the Chinese live up to these agreements. A common Chinese response to any mention of cyber-related issues emanating from their territory remains that "Cyberattacks are anonymous, cross-border and hard to trace."[8] However, for a country that so tightly controls its internet access to the outside world, these words fall on deaf ears.

This example of the Chinese hack of the Office of Personnel Management once again brings to the forefront that United States cyber policy of defense is inadequate to deal with the rapidly changing, technologically interconnected, global society we live and operate in. The debate on the potential response options to cyber hacks in the future is an issue that the United States will continue to face but currently is left with limited

---

*http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888?cb=logged0.08257161010988057* (accessed September 5, 2015).

[6] Office of the Press Secretary, *Fact Sheet: President Xi Jinping's State Visit to the United States*, The White House, (Washington D.C., 2015).

[7] Ibid.

[8] Devlin Barrett, Danny Yadron, and Damian Paletta, "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say", *The Wall Street Journal*, June 5, 2015, *http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888?cb=logged0.08257161010988057* (accessed September 5, 2015).

response options. Cyber policy today, with its minimal deterrent effect, will not impede other nations or non-state actors from engaging in cyber operations against the United States, and reflects the continuing evolution in the character of cyber warfare.

## RUSSIA

Russia has embraced the concept of offensive cyber operations. There have been numerous documented cases of the employment of cyber capabilities by Russia and groups sponsored by the Russian government during periods of increased tensions with other nation states. The Russians have used cyber prior to and during military operations effectively to further their overall goals. I will briefly discuss three cases of Russian offensive cyber operations to highlight the importance they place on these operations.

The first case which garnered international attention of Russian expertise in the conduct of offensive cyber operations against Estonia. Tensions between the governments of Estonia and Russia had been building since the disintegration of the Soviet Union in 1989. Estonia had been making great strides in assimilating into the international community and over the years had taken a series of actions to remove the last visible signs of Soviet oppression. In 2007, the Estonian Legislature had passed the Forbidden Structures Law, which did just that.[9] This law angered ethnic Russians in Estonia and caught the attention of the media and leadership back in Moscow which felt that something needed to be done.

[9] Richard A. Clark, and Robert K. Knake, *Cyber War The Next Threat to National Security and What To Do About it*, (New York: Harper Collins, 2010), pg 12-16.

Estonia is a highly interconnected country, even more so than the United States, which created serious cyber vulnerabilities.[10] As a result, when a fairly sophisticated denial of service attack hit Estonia, individuals were unable to connect to the internet, banking was taken off line, and communication links were jammed. This attack effectively severed Estonia's digital connection to the rest of the world. This series of actions precipitated a series of high level emergency meetings at the North Atlantic Treaty Organization to discuss the details of the incident and chart a way ahead to resolution.

The Russians were confronted and questioned about the cyberattack and they vehemently denied involvement. However, due to the complex nature of the attack and the banking and national communications nodes targeted; it left little doubt that the Russian government had knowledge and had provided at least tacit approval to the actors who carried out the operation. This was not the first time that the Russians used cyberattacks to respond to and defend their national interests, and it would not be the last. Ukraine was next.

The situation in Ukraine follows the same script that was executed in Estonia. Ukraine gained independence with the fall of the Soviet Union in 1989. Ukraine has generally maintained cordial relations with Russia, with tensions rising prior to presidential elections in the former territory. However, Russia first moved by seizing the Crimea to provide security to ethnic Russians that felt threatened by Ukrainians, and to recapture their Naval facility located on the peninsula. Follow-on action included irregular and proxy forces engaging in direct action in Ukraine. These series of

[10] Ibid, pg 13.

provocations set off alarm bells globally. NATO immediately called a series of meetings to gauge and work towards a solution to the situation.

According to Russian standard operating procedures, a series of denial of service attacks hit NATO and Ukraine. The attack was enabled by the exploitation of a "zero day" vulnerability, a vulnerability in software known only to the software developers and has not been patched, enabling an access point for exploitation by the attackers. Generally, once a denial of service attack occurs, the affected systems are taken off line and patches are applied to remedy the situation. In the case of Ukraine, this did not occur and the attack continued.[11]

Once again, it was suspected that the Russian government was responsible for the attack due to the ongoing tensions with Ukraine. The standard denial was issued from Russia, but the disavowal fell on deaf ears due to the complexity of the attack. If not directly involved in the attack, the Russian government supported the hackers who undertook the cyber offensive. The final example of Russian reliance on cyber involves cyber-enabled espionage.

In the summer of 2015 the unclassified email network of the Joint Chiefs of Staff was taken offline for weeks. Initially, there was no obvious reason for this action, and it slowed down the daily business of staffing those actions to support the United States military deployed across the globe. Then, in late summer, the Chairman of the Joint Chiefs of Staff, General Martin E. Dempsey, publically announced that the Russian

[11] Ellen Nakashima, "Russian hackers use 'zero-day' to hack NATO, Ukraine in cyber-spy campaign", *Washington Post*, October 13, 2015, https://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html (accessed October 20, 2015).

government was responsible for this action. Once again, due to the complexity of the actions taken to enable the penetration of the network, it was attributed to the Russians.[12] The public statement identifying the Russians as the perpetrators of the attack was the only known response, which tends to be the norm in espionage cases. However, this response was limited and generally has a minimal deterrent effect for future operations.

These three examples of Russian use of offensive cyber operations are representative of the importance Russia places on the future of cyber. The cyberattacks, synchronized with political and military action, afforded the time and space for Russia to achieve their objectives in support of their national interests. The motivation and characteristics of cyberattacks differ from actor to actor and from state to state. The North Koreans took cyberattack to a different level.

## SONY

*"Wow. Everyone caved, the hackers won. An utter and complete victory for them." Rob Lowe*[13]

In late November 2014, Sony Pictures Entertainment was poised to release the motion picture *"The Interview"*, a satire of two journalists that had been approached to assassinate the North Korean leader Kim Jong Un. However, as the date of the release approached, the computers at Sony became inoperable. Confidential files and unreleased movies were stolen; they had been attacked.

---

[12] Craig Whitlock, and Missy Ryan, "U.S. suspects Russia in hack of Pentagon computer network", *Washington Post*, August 6, 2015, https://www.washingtonpost.com/world/national-security/us-suspects-russia-in-hack-of-pentagon-computer-network/2015/08/06/b80e1644-3c7a-11e5-9c2d-ed991d848c48_story.html (accessed October 20, 2015).

[13] British Broadcasting Corporation, "The Interview: A guide to the cyber attack on Hollywood", *BBC*, London, 14 December 2014, http://www.bbc.com/news/entertainment-arts-30512032 (accessed October 20, 2015).

The immediate question asked was who was responsible, and what was the intent of these actions? The ability to definitely identify the source of a cyberattack is a manpower intensive and time consuming process. In performing the forensics of a cyberattack, successful techniques are on display and shared with the whole world. It becomes a painstaking exercise of deconstructing the attack, the malware used, the path taken, and finally the origin. North Korea helped the process along, by publically making demands to cancel the movie, and threatening attacks on the theaters that may have shown the movie. Sony finally made the determination to scrap releasing the movie. The game had changed, North Korea had successfully used a cyberattack to threaten the United States as well as coerce and intimidate the Sony Corporation to bend to their will.[14]

The official United States government statement in response to the incident was forceful, but unconvincing. President Obama stated that the response would come after careful determination of the time, place, and would be proportional.[15] It was assumed that a response would be cyber related, but how exactly to respond proportionally to a country that is isolated from the interconnected world is a challenge. The United States' response is still unknown. However, in late November 2014, the North Korean electrical grid went off line for nine and a one half hours, but attribution to the responsible party has still not been confirmed.[16]

---

[14] Department of Defense, Office of the Secretary of Defense, *DoD Cyber Strategy*. April 2015, (Washington, D.C., 2015), pg 4.
[15] David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony", *New York Times*, 19 December 2014, http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=1 (accessed October 20, 2015).
[16] Brian Fung, "North Korea's Internet outage was likely the work of hacktivists – but not the ones you might think", *The Washington Post*, December 23, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/23/north-koreas-internet-outage-was-likely-the-work-of-hacktivists-but-not-the-ones-you-might-think/ (accessed February 10, 2016).

On the surface the cyberattack was against a company, including their employees, and property. However, the Secretary of Homeland Security, Mr. Jeh C. Johnson, believes it is much more. It was an attack on the freedoms and way of life of the citizens of the United States.[17]

The example of North Korea's use of cyber warfare demonstrated the power of cyber and set a dangerous precedent within the international community. The world witnessed the United States powerless to effectively respond to the coercion, intimidation, and threat of attacks from North Korea. The tables had been turned on the United States who enjoys a significant military superiority. The asymmetric nature of cyber allowed a country that is at a disadvantage both militarily and economically to use a low cost capability to achieve its aims. The North Koreans effectively used Sun Tzu's dictum of attacking your opponents' strategy, which in this case is the United States cyber strategy of defense.[18]

The United States has enjoyed unprecedented success due to its reliance on cyber technology for every facet of daily life and business, but this reliance is also its greatest vulnerability. The Sony attack reinforced the need for a strong defense, while highlighting a lack of preparedness of not just the United States government, but most importantly, the need for corporations to plan and prepare to confront the growing threat that cyber presents to their individual business interests. The defensive nature of United States cyber policy has had a minimal deterrent effect against cyberattacks.

---

[17] David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony", *New York Times*, 19 December 2014, http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=1 (accessed October 20, 2015).
[18] Sun Tzu, *The Art of War*, translated by Samuel B. Griffith, (Oxford: Oxford University Press, 1963), pg 77.

A policy that articulates that the United States will take offensive cyber operations in response to a cyberattack would have a deterrent effect. It would induce a factor that would need to be accounted for in an adversary's calculus while determining their courses of action. This is an important fact. Currently, the United States policy is one of defense, the ability to secure the network to allow the government to operate in a degraded environment. The ability to protect the systems of the United States government is a difficult, if not an impossible undertaking, and needs to rely on deterrence and the threat of retaliation.[19] President Obama's vow of retaliation on North Korea is a testament to this fact. The North Koreans could have been deterred if the United States had a policy that clearly articulated offensive cyber operations.

The United States does place an importance on offensive cyber operations to secure and achieve national interests. In the next chapter, Stuxnet will show the potential that offensive cyber operations offer to the United States.

[19] David C. Gombert, and Martin E. Libicki, "Waging Cyber War the American Way." *Survival* Vol. 57, No.4 (July 2015), pg 14.

## CHAPTER: 5 STUXNET

*"Somebody crossed the Rubicon," Michael V. Hayden*[1]

In *Countdown to Zero Day*, Zetter details how the United States allegedly engaged in offensive cyber operations to sabotage the burgeoning Iranian nuclear program[2]. The Stuxnet operation is an excellent example of how lines of computer programming code can be used to create a kinetic effect, causing physical damage. It is natural for pundits to instantly revert to a parochial position to advocate that cyber alone can have immediate effects on an adversary. However, more importantly, Stuxnet showed that cyber, when integrated with other instruments of national power, created the time and space to provide the United States a decisive advantage in confronting the potential of a nuclear Iran.

Iran has desired to become a nuclear state for decades, but has dealt with repeated setbacks to achieving its aims. These include United States' sanctions as a result of the 1979 Islamic Revolution, and the bombing of nuclear related facilities by Iraq during the eight year Iran-Iraq War.[3] However, the goal of becoming a nuclear state remained and Iran looked to proliferation networks to gain the knowledge and materials to continue down the path of realizing their nuclear ambitions.

There was a real sense that the Iranians were undertaking enrichment activities critical in the development of nuclear weapons, while stating that their nuclear program was for

---

[1] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran" *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 (accessed September 10, 2015).
[2] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Crown, 2014), pg 1-4
[3] Ibid, pg 46.

purely peaceful purposes. The credibility of the United States had taken a major hit with the invasion of Iraq to disarm Saddam Hussein of weapons of mass destruction. The decision to preemptively invade Iraq had limited the options that the administration of George W. Bush could employ in dealing with a nuclear Iran. The international community was suspect of the claims of the Bush administration that Iran was developing nuclear weapons, and had little appetite for military action. As a result, sanctions were enacted to deal with Iranian illicit nuclear activities.[4] The sanctions, while an important step for slowing down Iranian nuclear ambitions, did not impede the Iranians.

Intense diplomatic efforts continued to build consensus that a nuclear Iran would pose a threat and eventually led the United Nations Security Council to pass resolutions related to Iranian illicit nuclear activities[5]. However, the Iranian nuclear program continued to move forward and there were growing concerns in the United States that Israel would take unilateral, preemptive action to attack Iranian nuclear facilities. Action needed to be undertaken in order to degrade and slow the Iranian program, and to simultaneously create breathing room for continued diplomatic efforts and allow the necessary time for sanctions to have an effect.

In January 2009, the President allegedly decided to use offensive cyber capabilities against enrichment-related facilities.[6] In early 2010, the International Atomic Inspection Agency, while conducting routine inspections on Iran's nuclear research facilities, noted

---

[4] Department of State, *Joint Comprehensive Plan of Action*, Vienna Austria, 14 July 2015, (Washington D.C., 2015), pg 2.
[5] Ibid, pg 2-3.
[6] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran" *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 (accessed September 10, 2015).

that the centrifuges used in the processing of uranium were failing at an alarming rate.[7] The inspectors and the Iranian scientists were at a loss to explain the reason for the failing centrifuges. When additional details of the cyber operation came to light, it was discovered that the Stuxnet malware was a complex and complicated intelligence operation to identify the network nodes, computers, and equipment associated with Iran's uranium enrichment program. Once the components of the enrichment system were identified, the operation morphed into one of sabotage, inflicting physical damage to the equipment used to process uranium in the enrichment cycle.[8]

While the positives of Stuxnet are many, there are also potential repercussions that need to be acknowledged. A considerable amount of concern was raised that if it became public knowledge that the United States conducted a cyberattack against Iran, it could result in the justification for other state and non-state actors to conduct them. An exploitation of a zero-day vulnerability generally tends to be a onetime use, and reveals the capability of the specifically designed cyber weapon to the world. The design information could provide an asymmetric advantage to an adversary to use in attacking the United States.

The United States was exposing itself to the same type of cyberattack since its critical infrastructure uses many of the same supervisory control and data acquisition components. During an interview with the news program 60 Minutes, then Director of the Central Intelligence Agency, Michael V. Hayden stated that "clearly, someone has

[7] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Crown, 2014), pg 1
[8] Ibid pg 3.

legitimatized this kind of activity as acceptable."[9] A reprisal attack from Iran never materialized, and to date the United States has not experienced a large scale cyberattack which created physical damage.

An additional concern was one of containment, ensuring that there was not spill over or leakage. The components targeted by Stuxnet were in a closed network of standalone systems not connected to the internet. However, if the Stuxnet malware were to migrate to the internet, the potential to affect users on a global scale was vast. Ultimately, the malware did indeed make its way to the internet and was instrumental in the deciphering of the specific coding techniques which allowed cyber security specialists to determine the intended components of the enrichment process that were targeted.[10]

The debate continues on exactly how long Iranian enrichment activities were set back by the Stuxnet operation, but there can be no mistake that it provided additional time for international sanctions to have an effect on the economy of Iran, and brought the Iranian government to the bargaining table. On 14 July 2015, the governments of the United States, the United Kingdom, France, Germany, the Russian Federation, China, the United States, and the Islamic Republic of Iran entered into an agreement to ensure that Iran's nuclear program will be exclusively peaceful. [11] There are many aspects of this historic agreement that remain contested but it may have never occurred if the use of offensive cyber operations had not been approved. However, it is important to restate that offensive cyber operations can be integrated with diplomatic, informational, and

---

[9] *60 Minutes*, "Stuxnet: Computer Worm Opens New Era of Warfare", CBS, June 4, 2012.
[10] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Crown, 2014), pg 167-168.
[11]. Department of State, *Joint Comprehensive Plan of Action*, Vienna Austria, 14 July 2015, (Washington D.C., 2015), pg 2.

economic instruments of power to create the time and space for a decisive advantage to the United States.

# CHAPTER 6: RECOMMENDATIONS

The United States needs a clearly articulated policy direction to support offensive cyberspace operations. In the various examples of cyberattacks, each instance produced the desired effect to the individual country or actor. This shows the increasing value of cyber, and portends a growing threat. To date, the United States has been averse to discussing offensive cyber operations in the public domain and has rarely spoken out about such operations.

First, the White House should direct the National Security Advisor to conduct a follow-up comprehensive whole of government review for cyber policy. The review should use the 2008 cybersecurity policy review as the starting point and apply those lessons learned from the Department of Defense cybersecurity strategies as well as the Department of Homeland Security cybersecurity initiatives.

As part of the final policy document, language detailing that the United States will conduct offensive cyber operations to protect the country and its national interests needs to be added. The focus should be on clarification on a set of easily understood thresholds that would necessitate the decision to conduct offensive operations. This can be accomplished by defining, as it applies to cyber, what constitutes an attack, aggression, or use of force in a situation of preemption. While the policy should seek to add clarity, the definitions should be vague enough to provide flexible responses to a multitude of situations.

A formal policy declaration coming from the White House lends credibility, removes ambiguity, and will support deterrence efforts. An updated policy will initiate a series of actions from the other departments to revise and update their individual strategies to maintain consistency across the government.

As the country enters a presidential election cycle there is little chance to accomplish this review prior to a new administration. However, it will have been nine years since an updated and revised national policy has been released. This policy update should be a priority.

The Department of Defense has maintained the momentum it started in 2011 and continued with the publication of the 2015 strategy. The document captures DoD views of the need for those offensive capabilities required to operate in cyberspace. However, the strategy could be more clearly articulated to state that offense should be the weight of effort. This change will not require major efforts. As discussed earlier, there are synergies that are gained in the development of defensive capabilities where vulnerabilities are identified and can in turn be exploited as offensive operations. Additionally, the creation and maturation of United States Cyber Command is a testament to this fact. It is a military organization that is focused on conducting both offensive and defensive operations. There remains ambiguity with the close relationship to the National Security Agency and the true purpose of the command.

The responsibilities of the Director of the National Security Agency and the Commander, United States Cyber Command should be separated. The size and scope of the responsibilities that Admiral Michael S. Rogers has in leading two large organizations is unwieldly. The dual-hatted nature of Admiral Rogers's responsibility creates

confusion and conflates the various lines of effort. A separation of responsibility would send a clear signal that there are military functions in cyber space that are separate from intelligence.

The habitual relationship that the National Security Agency has with the other members of the Intelligence Community would allow for sharing threat information of new actors, or signatures in cyberspace. The Director of National Intelligence would still perform the oversight function and serve and act as a clearing house for those intelligence-related matters and repo to those committees with oversight responsibility in Congress. This also has the potential to foster increased cooperation with the Department of Homeland Security to aid their mission of securing the nation's critical infrastructure by sharing cyber threat information with the private sector.

Finally, this would allow for greater focus and integration of both offensive and defensive cyber capabilities into joint operations. This action may necessitate an appointment of a new leader to one of the organizations, but the benefits clearly outweigh the associated costs. While the Senate Armed Services Committee would be involved in approval of any new leadership appointments, it is likely that Senator McCain, the Chairman of the committee, would support this measure.

There needs to be public acknowledgement by senior American leadership when the United States has conducted a cyber operation to thwart an impending attack, or in retaliation of a previous attack. As discussed in Chapter 3, President Obama vowed to respond to the North Korean cyberattack against Sony Pictures. The question still remains as to what was the United States response.

I'm not proposing that classified tactics, techniques, and tradecraft be compromised. Nor am I advocating that an acknowledgement be made public in response to a Chinese or Russian cyber-operation against the United States. There is a real possibility for a tit-for-tat game of escalation if that was to occur. However, because operations in cyberspace are only known to those adversaries being targeted, the United States will realize significant gains by increasing its flexibility to acknowledge an offensive cyber action, and in using the other instruments of national power when responding to cyberattacks. Public acknowledgement will provide senior decision-makers a range of options in choosing a path to respond. A declaratory offensive policy will not deter adversaries from attacking the United States, its interests, or allies, but the public acknowledgement of a response would benefit deterrence efforts. Once the United States used atomic weapons, it changed the calculus of adversaries; it deterred them from attacking. The same deterrent benefit could be gained by declaring the United States conducts offensive cyber operations.

These recommendations would require several meetings of the National Security Council to gain consensus and ensure that the Secretaries of the Departments understand the intent of the change in policy. The acknowledgement of offensive cyber operations codified in policy will remove ambiguity as to the true intent of operating in cyberspace. It will benefit the range of options that the leadership of the United States has available to use in responding in times of crisis and to ensure that the country's economic prosperity is secured.

# CHAPTER 7: CONCLUSION

Cyber has changed the strategic environment as we know it and will continue to evolve for the foreseeable future. Due to this technological change, conflict has become less dependent on geography than in the past and is moving to becoming borderless. It can allow a nation to impose its will on its adversary by removing the human element and violent characteristics typically associated with state on state conflict. Carl von Clausewitz, as he thought and reflected on war, came to the conclusion that war is an extension of politics. Cyber has already changed warfare, and the character of war has changed. Is the nature of war the next to change?

In Cyberwarfare, speed with constant adaptation to the ever changing environment is of the utmost importance; favoring the offensive provides an advantage. The United States places importance on cyber operations to secure the country and achieve its national interests, but more work needs to be accomplished.

While there is significant effort being made in regard to constructing a formidable defense, the ability to secure cyberspace is a never ending struggle. The current United States policy regarding cyber is focused on securing cyber defense. It is evident that there is a lot of work to be done to build consensus that offensive cyber operations is a part of the policy of the United States.

The various departments all acknowledge the fact that they will have to plan to operate in a denied and degraded cyberspace, which acknowledges to the fact that defense is not foolproof. Traditional models of deterrence do not apply to cyberspace; identifying the source and those responsible for an attack are long and time consuming

efforts, and in turn results in the loose of the potential deterrent effect or benefit being sought. Again, this leads to the perception that fortifying defenses to blunt attacks is cost-prohibitive. The policy of defense has not deterred nations, state-sponsored, and non-state actors from conducting cyberattacks against the United States, its citizens, and its interests. American leaders need to provide the policy and guidance to remove any ambiguity.

The United States lacks a clearly articulated policy to support offensive cyberspace operations. This policy direction may exist in classified channels, but the deterrent benefits of a clearly articulated publicly available policy are lost. There should not be any doubt that the United States has placed a priority on the development of offensive cyber capabilities. Vulnerabilities are discovered during the various phases of design of defensive capabilities, which immediately can be turned around and used for offensive purposes. Cyber budgets have increased exponentially to keep pace with the growing cyber threat; the assumption is that resources are not lacking.

The Chinese, Russians, and other state and non-state actors will continue to place an emphasis on increasing their cyber capabilities. Cyber provides an asymmetrical advantage to circumvent the United States' significant military capability. Cyber has played an important role in the prosperity that America enjoys, but is also its greatest vulnerability. A clearly articulated policy that stresses the importance of the offensive is required for the United States to defend itself in the ever changing nature of cyberspace.

Bibliography

Barrett, Devlin, Yadron, Danny, and Paletta, Damian, "U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say", *The Wall Street Journal*, June 5, 2015, http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888?cb=logged0.08257161010988057 (accessed September 5, 2015).

Brandes, Sean; "The Newest Warfighting Domain: Cyberspace**."** *Synesis: A Journal of Science, Technology, Ethics, and Policy* Vol. 4 (January 2013): G90-95.
British Broadcasting Corporation, "The Interview: A guide to the cyber attack on Hollywood", *BBC*, London, December 14, 2014, http://www.bbc.com/news/entertainment-arts-30512032 (accessed: October 20, 2015).

The Center for Strategic and International Studies; *U.S. Cyber Deterrence Declaratory Policies*, Washington DC, December 2015, http://csis.org/images/stories/tech/151214_Cyber_Deterrence_Declaratory_Policies.pdf, (accessed December 22, 2015).

Chaffetz, Jason, "The Breach We Could Have Avoided", *The Hill*, September 19, 2015, https://oversight.house.gov/op-ed/the-breach-we-could-have-avoided/, (accessed: October 5, 2015).

Clark, Richard A. and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Colling, 2010.

Department of Defense, Office of the Secretary of Defense, *DoD Cyber Strategy*, Washington, D.C., 2015.

Department of Defense *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*, Secretary of Defense Leon E. Panetta, New York, 2012.

Department of Homeland Security, Office of the Secretary of Homeland Security, *Blueprint for a Secure Cyber Future*, Washington, D.C., 2011.

Department of State, *Joint Comprehensive Plan of Action*, Vienna Austria, 14 July 2015, Washington D.C., 2015.

Executive Office of the President of the United States, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington D.C., 2009.

Fung, Brian. "North Korea's Internet outage was likely the work of hacktivists – but not the ones you might think", *The Washington Post*, December 23, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/23/north-koreas-internet-

outage-was-likely-the-work-of-hacktivists-but-not-the-ones-you-might-think/ (accessed February 10, 2016).

Gervais, Michael. "Cyber Attacks and the Laws of War" *Berkley Journal of International Law* Vol. 30, No. 2 (December 2012), 525-579.

Gompert, David C. and Martin Libicki. "Waging Cyber War the American Way." *Survival* Vol. 57, No. 4 (July 2015): 7-28, https://nduezproxy.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=108485663&site=ehost-live&scope=site (accessed November 10, 2015).

Harris, Shane. *@ War: The Rise of the Military-Internet Complex,* New York: Houghton Mifflin Harcourt, 2014.

Howell, Kellan, "U.S. will retaliate against China for OPM hacks", *The Washington Times*, August 1, 2015, www.washingtontimes.com/news/2015/aug/1/us-will-retaliate-against-china-for-opm-hacks/ (accessed: October 15, 2015).

Libicki, Martin C.; "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* Vol. 8, No. 2, Fall (December 2012): 325-340.

Nakashima, Ellen, "Why the Sony hack drew and unprecedented U.S. response against North Korea", *The Washington Post*, January 15, 2015, https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html (accessed February 10, 2016).

Nakashima, Ellen, "Cyber chief: Efforts to deter attacks against the U.S. are not working", *The Washington Post*, March 19, 2015, https://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html (accessed: October 20, 2015).

Nakashima, Ellen, "Russian hackers use 'zero-day' to hack NATO, Ukraine in cyber-spy campaign", *The Washington Post*, October 13, 2015, https://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html (accessed: October 20, 2015).

Office of the Press Secretary, *Fact Sheet: President Xi Jinping's State Visit to the United States*, The White House, Washington DC, September 25, 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed October 15, 2015).

Sanger, David E., "U.S. Decides to Retaliate Against China's Hacking", *The New York Times*, July 31, 2015, http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html (accessed September 5, 2015).

Sanger, David E, Schmidt, Michael S, and Perlroth, Nicole, "Obama Vows a Response to Cyberattack on Sony", *The New York Times*, December 19, 2014, http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=1 (accessed: October 20, 2015).

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran" *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 (accessed: September 10, 2015).

Sun Tzu, *The Art of War*, translated by Samuel B. Griffith, Oxford: Clarendon Press, 1963.

U.S. Government Accountability Office, "*Cybersecurity: national strategy, roles, and responsibilities need to be better defined and more effectively implemented*", U.S. Government Accountability Office. Washington D.C., 2013.

Von Clausewitz, Carl, *On War*, translated by Michael Howard and Peter Paret, New York: Princeton University Press, 1976.

Whitlock, Craig and Ryan, Missy, "U.S. suspects Russia in hack of Pentagon computer network", *The Washington Post*, August 6, 2015, https://www.washingtonpost.com/world/national-security/us-suspects-russia-in-hack-of-pentagon-computer-network/2015/08/06/b80e1644-3c7a-11e5-9c2d-ed991d848c48_story.html (accessed October 20, 2015).

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *JFQ: Joint Force Quarterly* No. 73 (April 2014): 12-9 https://nduezproxy.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=95531605&site=ehost-live&scope=site (accessed September 17, 2015).

Zetter, Kim**.** *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.

# Vita

Lieutenant Colonel Brian Sidari entered the Air Force in 1995 after receiving his commission through the Reserve Officer Training Corps at Kent State University as an intelligence officer. His operational tours were as the Director of Operations for the 390th Intelligence Squadron, Kadena Air Base, Okinawa, Japan and as the Commander of the 6th Intelligence Squadron, Osan Air Base, Republic of Korea. He has served in or deployed to U.S. European Command, U.S. Central Command, U.S. Pacific Command, Headquarters U.S. Air Force, and the Joint Staff. His most recent assignment was as the Executive Officer to the Vice Commander, Air Force Space Command, Peterson Air Force Base, Colorado Springs, Colorado.

Colonel Sidari holds a Bachelor of Arts in Political Science from Kent State University, a Master of Military Arts in Operational Art and Sciences, Air University, Maxwell Air Force Base, Alabama, and a Master of Science in Joint Campaign Planning and Strategy from the Joint Forces Staff College – National Defense University